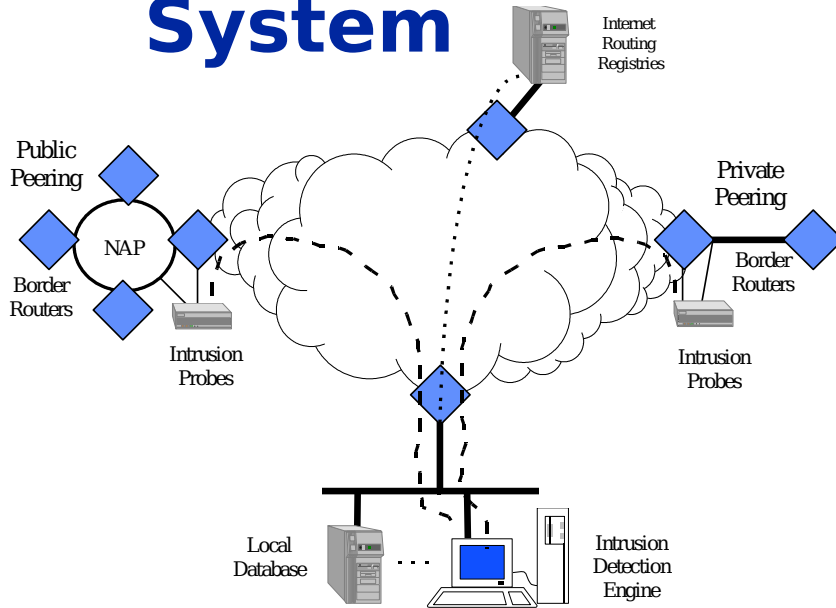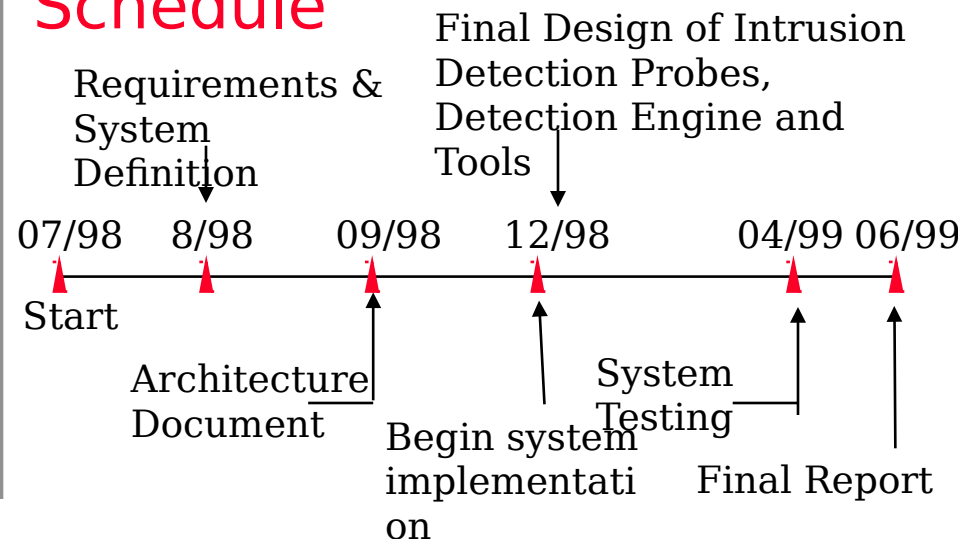# External Routing Intrusion Detection System

New Ideas

- A methodology for analyzing external routing behavior
- Novel approach for detecting external routing intrusion events
- Novel use of existing Routing Policy Databases

Impact

- Help NOC operators in troubleshooting BGPv4 problems due to malicious attacks or mis-configurations
- Provides a fast-deployable detection solution while a system of countermeasures becomes available
- Promote the use of Routing Policy Databases by National Backbone providers, ISPs and DSPs using BGPv4

Schedule

Final Design of Intrusion Detection Probes, Detection Engine and Tools

Requirements & System Definition

07/98   8/98   09/98   12/98   04/99 06/99

Start

Architecture Document

Begin system implementation

System Testing

Final Report

BBN Technologies, PI(s): Luis Sanchez, Stephen Kent